DETAILED ACTION

1. The response of 9/17/09 was received and considered.

2. Claims 3, 5-12 and 19-28 are pending.

EXAMINER'S AMENDMENT

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Michael Dunnam, Reg. No. 32,611 on 10/26/09.

The application has been amended as follows:

Please **REPLACE CLAIM 3 and CLAIM 22** with the **FOLLOWING**:

3. (Currently Amended) A method of detecting surveillance probes on a computer communications network, comprising:

receiving a plurality of messages from a data sensor located at a network audit point, said data sensor sampling data packets on said computer communications network and outputting said messages, each of said messages describing an event occurring on said communications network;

processing said messages to form extrapolated connection sessions from said sampled data packets from which to determine a connection source that initiated the connection session by clustering packets exchanged in respective directions over a connection between addresses associated with a connection identifier for said connection, said addresses including an address of said connection source and a destination address, and clustering packets that are a) within a specified time period where the

source and destination addresses are not predetermined, (b) have certain flags set, or c) have source and destination addresses that are not predetermined but have similar characteristics; and

detecting a surveillance probe by:

grouping said connection sessions into a plurality of groups of related connection source addresses;

scoring each group based on at least a quantity of attack destinations; and

generating an alert for each group whose score is greater than an empirically derived threshold.

22. (Currently Amended) A system for detecting surveillance probes on a computer communications network, comprising:

a data sensor located at a network audit point adapted to sample data packets on said computer communications network and to output messages, each of said messages describing an event occurring on said communications network; and

a processor that processes said messages to form extrapolated connection sessions from said sampled data packets from which to determine a connection source that initiated the connection session by clustering packets exchanged in respective directions over a connection between addresses associated with a connection identifier for said connection, said addresses including an address of said connection source and a destination address, and clustering packets that are a) within a specified time period where the source and destination addresses are not predetermined, (b) have certain flags set, or c) having have source and destination addresses that are not predetermined but have similar characteristics, and that detects a surveillance probe by grouping said connection sessions into a plurality of groups of related

connection source addresses, scoring each group based on at least a quantity of attack destinations, and generating an alert for each group whose score is greater than an empirically derived threshold.

Allowable Subject Matter

4. Claims 3, 5-12 and 19-28 are allowed.

5. The following is an examiner's statement of reasons for allowance:

a. Regarding claims 3 and 22, the prior art has been discussed in the previous correspondence. Further, the Baba reference is cited for teaching sensing packets, grouping them by source and scoring the groups based on the number of attack destinations (particularly cols. 12-13). The Givoly reference is cited for teaching sensing packets, grouping by source aggress and maintaining sessions (particularly col. 4). The Robert and Malan references are cited for teaching the detection of SYN-ACK attacks. However, the prior art of record fails to teach or disclose, either alone or in combination, receiving messages resulting from packets and describing events on a network, processing the messages to form extrapolated connection sessions from the sampled data packets form which to determine a connection source that initiated the connection session by clustering packets exchanged in respective directions over a connection between addresses associated with a connection identifier for said connection, said addresses including an address of said connection source and a destination address, and clustering packets and detecting a surveillance probe by grouping the connection sessions into a plurality of groups of related connection source addresses, scoring each group and generating an alert for each group, in combination with the other elements of the claims and as described in the specification, particularly ¶70.

b. Claims 5-12, 19-21 and 23-28 are allowable based on their dependence.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J. SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571)272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

October 26, 2009
/Michael J Simitoski/
Primary Examiner, Art Unit 2439